Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of Section 304 of the Telecommunications Act of 1996	)	CS Docket No. 97-80
	)	
	)	
Commercial Availability of Navigation Devices	)	PP Docket No. 00-67
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	

COMMENTS OF BEYOND BROADBAND TECHNOLOGY, LLC

William D. Bauer
Beyond Broadband Technology, LLC
1140 10th St
Gearing, NE 69341

June 14, 2010

SUMMARY

"Whatever happened to downloadable security?" That question, pointedly posed by Commissioner McDowell in his separate statement, should serve as the starting point in the Commission's consideration of interim modifications to the CableCARD regime that would apply while it pursues the establishment of a successor to that regime. After all, even as the Commission was pushing forward with the implementation of the CableCARD regime in 2005, it acknowledged that "the development of set-top boxes and other devices utilizing downloadable security is likely to facilitate the development of a competitive navigation device market [and] aid in the interoperability of a variety of digital devices."

Yet, the underlying (but unstated) assumption of the Commission's Fourth Further Notice of Proposed Rulemaking ("*FNPRM*") and the related AllVid Notice of Inquiry ("*AllVid NOI*") is that the only way to "reform" the CableCARD regime is to abandon separable security and replace it with a separable navigation approach. **That assumption, however, ignores the fact that downloadable security exists and is available now.**

Beyond Broadband Technology LLC ("BBT") has spent the last six years developing and refining an open-standard, platform-agnostic downloadable security solution ("*The BBTSolution*™") that offers a viable low-cost substitute for expensive CableCARD devices. While various marketplace and regulatory obstacles (unrelated to technical issues) have impeded our efforts to fully deploy this technology, we are pleased to publicly announce that *The BBTSolution*™ recently passed a major milestone – a fully operational set-top integrated with *The BBTSolution*™ successfully completed a security assessment audit conducted by Telecordia Technologies, Inc. (formerly Bell Labs).

Downloadable security in the form of *The BBTSolution*™ not only exists, it also is fully capable of serving the goals of Section 629 of the Communications Act and the National Broadband Plan – provided the Commission learns from, rather than repeats, the mistakes of the past. In particular, *The BBTSolution*™ meets the Commission's goal for a low-cost device capable of facilitating the development of a robust competitive marketplace for navigation devices. The secure microchip, including the license, is priced at $5.00. The license protects the security of the device, but places no other restraints on licensees. In short, BBT is now able to offer the various industries, consistent with the Commission's objectives, something they have never really experienced before – an approach to the integrated box issue that solves an industry-wide problem, responds to a government mandate, yet does not interfere with or dictate the competitive business plans of the diverse parties involved.

In the *FNPRM*, the Commission has asked for comment both on the general issue of "reforming the CableCARD system" and on specific proposals for such reform. While "reform" of the CableCARD regime is essential (and long overdue), the Commission should be cautious not to throw the baby out with the bathwater. The Commission's separable security approach is on the verge of success. But by signaling that the separable security approach will be supplanted by a separable navigation approach, the Commission is effectively putting an end to any interest in the consumer electronics industry for any devices utilizing separable security, rendering the proposed short-term reforms superfluous at best. At worst, it may completely stall out the progress that finally is being made towards the deployment of an efficient and flexible downloadable security solution that represents the type of innovative thinking that up until now the Commission has encouraged.

With respect to the specific proposals set forth in the *FNPRM*, BBT agrees that during the transition to a successor to the CableCARD regime, the interests of consumers who have purchased CableCARD devices need to be protected. But pricing reforms are meaningless given that the Commission's pronouncements effectively are squelching the market for both CableCARD-enabled devices and for the production of CableCARDs embedded with downloadable security. While there is no inherent technical difficulty in embedding *The BBTSolution*™ secure microchip in the CableCARD form factor, it would be prohibitively expensive to manufacture totally new CableCARDs for systems employing the BBT downloadable security solution in the face of the Commission's proclaimed intention to adopt the AllVid device approach as a successor to the CableCARD regime.

BBT also agrees that the Commission should adopt a more flexible approach with respect to its interface requirement, allowing cable operators to choose among IEEE 1394, Ethernet, Wi-Fi, and USB interfaces. However, we disagree with the Commission's specification of USB 3.0 as the approved USB interface. Many chip manufacturers have yet to convert to USB 3.0 and there are numerous video end-user devices employing USB 2.0. While there is no indication that the cable industry will not upgrade to USB 3.0 when that interface becomes the norm, there also is no reason to delay the introduction of compatible devices in the meantime.

We have no reason to comment specifically on the *FNPRM's* proposals regarding CableCARD installations. In general, downloadable security is accomplished in the chip set built into the device. The same is true for IP "over the top" delivery or IPTV applications; all of these devices, once *BBTSolution*-enabled, could then have whatever "conditional access" the operator or programmer was using downloaded to them. There would be no distinction between devices purchased by consumers and devices provided by the cable operator and "installation,"

to the degree it was required, would be hooking the physical cable connection, modem Wi-FI, etc. to the given device. In a two-way system all security functions would then be automatic; in a one-way system, the consumer may have to make a one-time call to the system offices to activate the security (the same approach used in the initial cable modem installations).

As a general comment with respect to the *FNPRM's* proposals regarding multi-stream CableCARDs and Switched Digital Video, BBT notes again that mandating significant technical changes for the cable industry in an interim effort to make the CableCARD regime work better while simultaneously acknowledging that the separable security approach is going to be abandoned makes little sense and creates an almost impossible hurdle for new technology entrants. It also is inconsistent with Congress' expectation that the implementation of Section 629 would not impede technological innovation. These issues, along with other issues raised in the *FNPRM* are more appropriately considered in the companion *AllVid NOI* proceeding.

With the above thought in mind, BBT notes that *The BBTSolution*™ allows a single secure communications path to deliver multiple signals. Therefore, the issue would not be whether the "card" could accommodate more than one "stream"; rather, the issue would be whether the consumer device is equipped with multiple tuners – a decision for equipment manufacturers. As for Switched Digital Video and the associated TiVO suggestion regarding return path communications, the very asking of these questions illustrates the fundamental flaw in the Commission's approach. Sorting out these complex technical questions in the context of trying to create "interim steps as an important bridge to the implementation of a successor technology" could end up resulting in the construction of an interim bridge to nowhere.

Finally, the Commission's proposal to adopt an across-the-board exception for low-cost, limited capability devices in place of its case-by-base waiver approach is not just a "limited

modification" of the current rules as the Commission claims. Rather, it would essentially eliminate the "separable security" requirement for all one-way navigation devices. The Commission appears to be operating under the assumption that the high cost of devices with separable security necessitates broad relief from the current rule so as to facilitate the accomplishment of the goals of Section 629 and the National Broadband Plan. This assumption is mistaken. Today, almost all cable systems, large and small, are delivering high definition programming, and broadband offerings have become nearly ubiquitous. **More importantly, cable systems that the Commission assumes could not afford to offer digital service without a non-compliant device have received bids for compliant devices from established set-top box manufacturers at prices in exactly the same range as the prices quoted for non-compliant DTAs.**

The adoption of a broad, across-the-board exception to the current rules would have severe consequences for companies such as BBT that have responded to the Commission's past statements encouraging the development of downloadable security solutions. The developers of *The BBTSolution*™ are themselves small operators and thus are totally sympathetic to the needs of small systems. That is why we have devoted so much time and effort to designing a downloadable security solution that can more than double current bandwidth usage, can reduce headend costs, and can provide operators with the ability to provide advanced services. But if the Commission changes its rules, these benefits will be delayed or lost and, paradoxically, instead of moving forward, the industry will largely stay where it is. This is not the ultimate objective sought by Congress or the Commission.

TABLE OF CONETENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of Section 304 of the Telecommunications Act of 1996	)	CS Docket No. 97-80
	)	
	)	
Commercial Availability of Navigation Devices	)	PP Docket No. 00-67
	)	
Compatibility Between Cable Systems and Consumer Electronics Equipment	)	

COMMENTS OF BEYOND BROADBAND TECHNOLOGY, LLC

Beyond Broadband Technology, LLC ("BBT") hereby submits the following comments on the Fourth Further Notice of Proposed Rulemaking ("*FNPRM*") in the above-captioned proceedings.[1] In his separate statement on the *FNPRM* and the Commission's companion Notice of Inquiry on the "AllVid" device ("*AllVid NOI*"), Commissioner McDowell pointedly asked, "whatever happened to downloadable security?"[2] The answer is that, despite barriers thrown in its path by regulatory as well as market forces, downloadable security has become a reality. Indeed, BBT is pleased publicly announce that it recently passed a major milestone: a fully operational set-top

---

[1] *Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronics Equipment*, Fourth Further Notice of Proposed Rulemaking, CS Docket No 97-80, PP Docket No. 00-67 (rel. April 21, 2010) ("*FNPRM*"). *See also Video Device Competition; Implementation of Section 304 of the Telecommunications Act of 1996: Commercial Availability of Navigation Devices; Compatibility Between Cable Systems and Consumer Electronics Equipment*, Notice of Inquiry, MB Docket No. 10-91, CS Docket No. 97-80, PP Docket No. 00-67 (rel. April 21, 2010) ("*AllVid NOI*").

[2] *Id.* (Statement of Commissioner McDowell).

box integrated with BBT's downloadable security solution ("*The BBTSolution*™") successfully completed a security assessment audit conducted by Telcordia Technologies, Inc. (formerly Bell Labs). The successful testing of the *The BBTSolution*™ means that the Commission has at hand the long-awaited technology that offers the best chance of achieving the various policy objectives that motivated it to revisit the CableCARD regime – provided, however, that the Commission learns from, rather than repeats, the mistakes of the past.

INTRODUCTION AND BACKGROUND

Over five years ago, BBT came to the same conclusion that the Commission has tentatively reached in the *FNPRM/AllVid NOI*: that the policy objectives articulated by Congress in Section 629 were not going to be achieved through the deployment of CableCARD technology. In an effort to find a more workable alternative, BBT's founders looked to the cable modem model – a flexible, user-friendly device that within a relatively short time became a nearly ubiquitous part of the telecommunications landscape. What BBT settled on was an open standard downloadable security solution responding to the need for separable security and flexibility in navigation devices.

The decision to focus on developing a downloadable security solution as a successor to the CableCARD regime was driven in part by the Commission's own repeated endorsement of that idea. Indeed, even as the Commission was pushing ahead in 2005 with the implementation of the CableCARD regime, it was acknowledging that the "development of set-top boxes and other devices utilizing downloadable security is

likely to facilitate the development of a competitive navigation device market [and] aid in the interoperability of a variety of digital devices."[3]

With these words of encouragement to guide them, the three cable operators that founded BBT set about the task of developing an open standard downloadable security solution. By late 2006, BBT was able to inform the Commission that it had successfully developed a "unique, highly secure" downloadable security solution capable of providing "a viable low-cost substitute for expensive CableCARD devices."[4] As BBT explained at the time, its downloadable security design "will allow operators to quickly and inexpensively migrate from analog to digital transmission, including high definition, thus maximizing bandwidth utilization and assuring their ability to compete with both DBS and other technologies. It will also aid in the Commission's goals of completing the digital transition and expanding broadband Internet availability."[5]

Since 2006, BBT has been working assiduously to refine and bring to market a downloadable security solution that will help fulfill the Commission's goal of "ensur[ing] the commercial availability of navigation devices used by consumers to access the services of multichannel video programming distributors."[6] And we have been

---

[3] *Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices*, CS Docket No. 97-80, Second Report and Order, 20 FCC Rcd 6794, 6810 (2005).

[4] Letter from Seth A. Davidson, Counsel for BBT to Marlene Dortch, Secretary, Federal Communications Commission, CS Docket No. 97-80 (December 22, 2006), attaching Letter from BBT to Kevin Martin, Chairman, Federal Communications Commission dated December 21, 2006).

[5] *Id.*

[6] *FNPRM* at ¶ 1.

successful. *The BBTSolution*™ downloadable security design is platform agnostic. It can work with cable, DBS, broadcast, and broadband Internet protocols, among others. It works on both two-way and one-way communications platforms, and it does not require a "trusted authority," which has been one of the principal roadblocks to the adoption of non-integrated security by competitors.[7] Most significantly, it is the only downloadable security system successfully designed to provide an open standard, or specification, thereby allowing any commercial manufacturer to incorporate the secure microprocessor in their consumer electronics equipment and to download multiple, non-proprietary "conditional access" software and other "middleware" including electronic program guides.

There is no question that bringing the BBT downloadable security solution to market has taken longer than anyone expected. But the hurdles that BBT has had to overcome were largely unrelated to the technical breakthroughs required for a successful system; those have been in place for a while. Rather, BBT had the misfortune of bad timing – trying to introduce an innovative new technology in the midst of the worst economic downturn in a generation. BBT also had to deal with hurdles associated with its size and the fact that it was breaking new ground in an area that has been dominated by just a few players.

For example, BBT faced what often is referred to as the problem of "not invented here" (or "NIH"). The NIH phenomenon can bedevil efforts to reach an industry-wide

---

[7] A "White Paper" more fully explaining the technology is attached hereto. Note particularly, that *The BBTSolution*™ separates the creation of a secure communications path from "conditional access" to particular channels, data, or information. The "conditional access" conditions are downloaded after the secure communications path is established, thus giving all information or data providers' total control over what form of "conditional access" or "digital rights management" or both they wish to use.

consensus to embrace a particular technology; it simply is the nature of the competitive beast that companies do not want to passively accept the technology of a rival. Similarly, industry consortia often encounter difficulties in trying to satisfy the multiple and often conflicting desires of their members. And when more than one industry is involved, as is the case here, business plans and interests often conflict.

It is for that reason that BBT chose to try to stay independent of all the "major players" and create a minimalist technology that would accomplish the Commission's goals without interfering with the individual business decisions of the various parties. In particular, as noted above, *The BBTSolution*™ is designed to be "open." It creates a non-integrated security platform upon which each player can create and download its own conditional access and middleware to achieve whatever business model it chooses to pursue. It is inexpensive. The secure microchip including the license is priced at $5.00. The license protects the security of the device, but places no other restraints on licensees. Once the market is primed, BBT does not intend to be involved in the manufacture of end-user devices at all. In sum, what BBT has tried to offer the various industries, consistent with the Commission's objectives, is something they have never really experienced before – something that solves an industry-wide problem, responds to a government mandate, yet does not interfere with or dictate the competitive business plans of the diverse parties involved.

Another hurdle that BBT has had to deal with is its size. BBT is not one of the "known big players" which inherently makes getting a foothold in this arena difficult. However, BBT also firmly believes that its small size was crucial in creating an environment in which consensus on uniform technology might develop. BBT has not

tried to dictate any business plan by the technology we have developed. Indeed, BBT refers to *The BBTSolution*™ as "minimalist" because it takes one key element that has created the most significant barrier for system operators, programmers, and consumer electronics manufacturers – the establishment of a secure communications path – and leaves all the other business and policy differences to the market (or regulation, whichever occurs first.)

Finally, and in many ways most significantly, BBT has had to overcome uncertainty arising out of the Commission's decision-making. Even after the Commission acknowledged that *The BBTSolution*™ was compliant with its rules, the agency's ad hoc waiver-based regulatory approach has fostered an environment in which operators were reluctant to commit to a long-term solution such as the one offered by BBT.[8]

The good news is that BBT has shown that it can overcome the conditions that previously slowed the deployment of *The BBTSolution*™. We have shown that we are serious and in the game for the long haul notwithstanding our size and the uniqueness of our approach. We have, through field and laboratory testing, demonstrated that our approach works. And with the economy beginning to turn around, interest in what we have created and its enormous potential appears to be growing. The one issue that still

---

[8] The Commission has expressly acknowledged that *The BBTSolution*™ can be deployed by MVPDs without having to obtain a waiver of the separable security rules. Public Notice, "*Commission Reiterates That Downloadable Security Technology Satisfies the Commission's Rules on Set-Top Boxes and Notes Beyond Broadband Technology's Development of a Downloadable Security Solution*," 22 FCC Rcd 244 (2007). *See also In the Matter of Comcast Corporation's Request for Waiver of Section 76.1204(a)(1) of the Commission's Rules*, Memorandum Opinion and Order, 22 FCC Rcd 228, ¶ 34 (2007) (indicating that an operator deploying BBT's downloadable security solution would not need a waiver of the integration ban).

poses a potential overhang is the uncertainty created by the Commission's actions (and inaction) in implementing Section 629, including uncertainty arising out the *FNPRM* and the *AllVid NOI.*

In the *FNPRM*, the Commission has asked for comment both on the general issue of "reforming the CableCARD system" and on specific proposals for such reform. In the discussion that follows, BBT explains that while "reform" of the CableCARD regime is essential (and long overdue), the Commission should be cautious not to throw the baby out with the bathwater. The issue of what long-term reform of the CableCARD regime should look like is teed up in the separate *AllVid NOI.* Moving ahead with short-term "reforms" of the CableCARD regime while the outcome of the *AllVid NOI* (and of any rulemakings arising from the *AllVid NOI*) remains uncertain would, we believe, slow down or completely stall out the progress that finally is being made towards the deployment of an efficient and flexible downloadable security solution that represents the type of innovative thinking that up until now the Commission has encouraged.

DISCUSSION

I. REFORMING THE CABLECARD REGIME SHOULD BE UNDERTAKEN AFTER, NOT BEFORE, THE ISSUES RAISED IN THE *ALLVID NOI* ARE FULLY RESOLVED.

If one was looking for a model of how not to go about setting public policy, one would have to look no further than the history of the Commission's efforts to implement Section 629 of the Communications Act. For well over a decade, those efforts have been characterized by delay, litigation, uncertainty, exceptions, and waivers. Not surprisingly, the end results have satisfied no one – not the cable industry, not the consumer electronics industry, not the public, and not the Commission.

Yet, almost despite itself, the Commission's separable security approach is finally on the verge of success. By having left open the door for technological innovation (and by the industries having picked a particularly clumsy approach to separable security in the CableCARD solution), the Commission encouraged the development of a downloadable security solution that is far more efficient, far more flexible, and, importantly, far less costly than the CableCARD regime. Yet, it appears that the Commission is now poised to snatch defeat from the jaws of victory by once again changing course and by proposing short-term "reforms" of the CableCARD regime that will undermine the accomplishment of the goals of Section 629.

BBT intends to file separate comments in the *AllVid NOI* proceeding wherein we will go into more detail as to why we believe that the fostering of a downloadable security solution is far more likely to achieve most of the Commission's objectives in a shorter time frame than the Commission's latest idea, which essentially seeks to substitute "separable navigation" for the current approach of "separable security." We believe changing directions in this manner will be an incredibly complex and expensive road to travel, and one that will take far more time than the Commission anticipates.

For now, however, in this proceeding, the point can only be made again that no matter how long it has taken to get to this juncture regarding downloadable security, we have now reached it. According to the Commission, the purpose of the *FNPRM* is to explore reforms to the current CableCARD system "while the Commission works to establish a successor solution for retail navigation device compatibility with MVPD services."[9] An open standard downloadable security solution that is fully compliant with

[9] *FNPRM* at ¶ 12.

the Commission's existing rules exists and is technically capable of becoming the "successor to the CableCARD regime." Indeed, *The BBTSolution*™ offers a clear path towards the fulfillment of the aspirations articulated throughout the long history of the Commission's efforts to implement Section 629.

Unfortunately the short term reforms that the Commission has proposed pending a decision on a long term "successor" to the CableCARD regime may block this path. The clear import of the *FNPRM* is that the successor to the CableCARD will be the AllVid device. However, by signaling that the separable security approach will be supplanted by a separable navigation approach, the Commission is effectively putting an end to any interest in the consumer electronics market (to the degree there was any) for the continued development or manufacture of devices utilizing separable security – either in the CableCARD format or otherwise – rendering the short-term reforms it is proposing superfluous at best, and destructive to alternative technologies at worst.

Specifically, new designs for MVPD hardware take, on average, 18 months to move from the drawing board to full consumer production. We and many others far larger have tried to pare down that time frame to little effect. BBT is in total agreement with the Commission and most other commentators that technical developments in the last decade have overtaken the CableCARD form factor. But that does not mean the Commission should abandon "separable security" as what may be the best mechanism for ultimately reforming and modernizing the set-top box (or consumer electronics end-user device) market.

For example, the newest TiVo devices as well as many new Blu-ray players and video game consoles already have USB interfaces. The BBT downloadable security

solution has been successfully tested using that form factor. Separable security would still work with these devices; it would just work in a format (USB) that has become ubiquitous, unlike the CableCARD which uses a form factor (PCMCIA) which has essentially been abandoned in most other consumer settings.

The challenge of introducing any "new" technology is the relative cost and "pain" of the transition to industries and to consumers. It is our belief that virtually all cable systems could migrate from one form factor (CableCARD) to the other (downloadable security with either embedded secure microchips in new devices, or in some cases use of existing alternative interfaces) without major disruption. Many existing conditional access designs can be modified to be downloadable. In those systems where that is not the case, employing either simulcrypt or simulcast approaches would allow for a measured migration without the need to abandon equipment already in the field.

Indiscriminate "reforms" to the existing rules – which will effectively gut them – could well jeopardize the progress that has in fact been made toward the Commission's goals.[10] The Commission should do nothing in this proceeding that would obstruct the

[10] As is noted in the "White Paper" attached hereto, Congress and the Commission made clear that they did not want to interfere with, and indeed wanted to promote technical innovation. Recognizing the BBT downloadable security approach as a compliant technical effort for "separable security" has been significant in that respect. The Commission can take great credit for promoting the development of a new technology that now has the potential to be used not only in cable set-top boxes, but also on computers using the Internet, on DBS, and even on DTV as well as IPTV. We are no longer dealing solely with the issue of cable television entertainment delivery by set-top boxes. The decisions that the Commission makes in this proceeding (and the associated *AllVid NOI* proceeding) either to encourage or to slow down technical developments in separable security will have a direct impact on other critical areas such as the security of electronic health care records and Internet privacy and security.

true progress that finally is being made in the development and deployment of downloadable security.

II. COMMENTS ON SPECIFIC PROPOSALS IN THE *FNPRM*

A. CableCARD Pricing and Availability

The *FNPRM* proposes rules requiring cable operators to charge "equivalent and transparent" prices for CableCARDs.[11] While we agree that, during the transition to a successor to the CableCARD regime, the interests of consumers who have purchased CableCARD devices need to be protected, the issue of pricing reforms is meaningless in the context of innovative new technologies such as *The BBTSolution*™ given that the Commission's pronouncements regarding its intention to abandon separable security have effectively squelched the market for the manufacture not only of CableCARD-enabled devices but also CableCARDs embedding new security solutions such as *The BBTSolution*™.

Since a set-top box or other form of receiving equipment enabled with BBT's downloadable security solution is compliant with the Commission's "separable security" rules without using a CableCARD, the deployment of "BBT CableCARDs" would be necessary only for those few purchasers who have CableCARD enabled independently purchased devices. There is no inherent technical difficulty in embedding *The BBTSolution*™ secure microchip in the CableCARD form factor and BBT is prepared to support that effort so that consumers who have purchased CableCARD-enabled devices

[11] *FNPRM* at ¶ 15.

can continue to use those devices if the system to which they subscribe opts to utilize *The BBTSolution*™.[12]

However, while the dominant suppliers of set-top boxes in the United States today already have manufactured CableCARDs for distribution by system operators, and should continue to do so, it is unlikely that manufacturers of CableCARDs would initiate new production lines of CableCARDs to support competing alternative technologies in the face of pronouncements from the Commission that a successor to the CableCARD regime is going to emerge. To do so would cost hundreds of thousands or millions of up-front dollars with very little prospect for the eventual sale or use of the resultant manufactured cards.

More specifically, based on the current adoption of CableCARDs in the existing dominant set-top box systems (not those used in leased boxes by the operator, but those used by consumers who have purchased independent "host" devices), we can extrapolate that fewer than 25 customers in a 5000 subscriber system would likely seek the CableCARDs. That is insufficient to create a market. The current dominant manufacturers of CableCARDs happen to also be the current dominant suppliers of set-top boxes and proprietary conditional access systems. There is no indication that they are willing to virtually "custom produce" the very small numbers of CableCARDs that any

[12] *The BBTSolution*™ approach respects the underlying desire of the consumer electronics industry to be able to build and sell a "common reliance" design. *The BBTSolution*™ secure microchip is backward compatible with the "common reliance" CableCARD form factor. A BBT CableCARD will be made available once commercial adoption of *The BBTSolution*™ is established. Thus, the consumer electronics industry has full flexibility to design and sell both CableCARD-enabled "common reliance" devices as well as devices employing innovative alternative technologies. The consumer market is replete with examples of this approach, such as the CD/DVD/Blu-ray or AM/FM/HD radio devices now sold individually and in combinations nationwide.

new entrant would be called upon to provide in the first year to 18 months of distribution. And if the Commission follows through with the adoption of the AllVid device approach as a successor to the CableCARD regime, the market window would then close completely. We do not believe that the Commission intends the release of the *FNPRM* and associated *AllVid NOI* to foreclose new technology and new entrants; however that is one of the potential outcomes unless the Commission recognizes the impact of its own actions.

B. Interface Devices

The Commission notes in the *FNPRM* that waiver requests relating to the requirement that IEEE 1394 interfaces be included on all high-definition set-top boxes have made a "compelling case" that "IP connectivity will provide consumers with the functionality that the IEEE 1394 interface requirement was intended to provide."[13] Accordingly, the Commission proposed to modify its interface requirement to allow cable operators to include on high-definition set-top boxes any of (i) an IEEE 1394 interface; (ii) an Ethernet interface; (iii) Wi-FI connectivity; or (iv) USB 3.0.[14] BBT fully supports the notion that there should be more flexibility in the type of interface device used on high-definition set-top-boxes.

The Commission's proposals, borne out by the multiple waiver requests it has received with respect to the IEEE 1394 interface requirement, illustrate the pitfalls of "picking winners" in technology standards. The IEEE 1394 requirement adds an

[13] *FNPRM* at ¶ 19.

[14] *Id.* at ¶ 20.

expensive burden without commensurate gain. The alternative interfaces proposed, Ethernet, Wi-Fi or USB, would lower costs and assist in creating a more functional consumer device. We take issue, however, with the Commission's specification of USB 3.0 as the approved USB interface. As the Commission is aware, USB 3.0 is the newest iteration of the USB interface. It is very good, and it is likely, in the future, to be widely adopted as have the earlier versions. But to require all cable-distributed HD set-top boxes to have the 3.0 version today if they choose to use a USB interface would, once again, create an unnecessary burden. Major chip manufacturers have yet to convert to the 3.0 version. Set-top boxes with USB interfaces would thus face lengthy delays getting to market. Meanwhile there are numerous video end user devices that employ USB 2.0, much to the delight of consumers. Cable operators should be allowed to offer those devices as well. There is no indication that the industry would not upgrade to USB 3.0 when that becomes the norm. There is no reason to delay introduction of compatible devices in the meantime.

C. CableCARD Installation, Multi-Streaming and Switched Digital Video

Three other proposed "reforms" of the current CableCARD rules on which the Commission is seeking comment include (i) whether to require cable operators to allow consumers to self-install CableCARDs in retail devices if the operator allows consumers to self-install leased boxes; (ii) whether to require cable operators to offer multi-stream CableCARDs; and (iii) whether (as suggested by TiVo) to require cable operators to

allow retail CableCARD devices to receive out-of-band communications from the cable head-end and transmit out-of-band communications to the headend over IP.[15]

As a general comment with respect to the *FNPRM's* proposals regarding multi-stream CableCARDs and Switched Digital Video, BBT notes again that mandating significant technical changes for the cable industry in an "interim" effort to make the CableCARD regime work better while simultaneously acknowledging that the regime is likely to end soon makes little sense, and creates an almost impossible hurdle for new technology entrants. It also is inconsistent with Congress' expectation and intent that the implementation of Section 629 would not impede technological innovation. These issues, along with other issues raised in the *FNPRM*, are more appropriately considered in the companion *AllVid NOI* proceeding than as "interim" reforms of the existing CableCARD rules.

With the above thought in mind, BBT notes that *The BBTSolution*™ allows a single secure communications path to deliver multiple signals. Therefore, the issue would not be whether the "card" could accommodate more than one "stream"; rather, the issue would be whether the consumer device is equipped with multiple tuners. That is a decision for equipment manufacturers, and is not inherently limited by downloadable security. In the broadband, "over the top" context, each programmer could potentially be "tuned" separately (going from one URL to another would be the equivalent of changing channels).

As for Switched Digital Video and the associated TiVo suggestion regarding return path communications, the very asking of these questions illustrates the

[15] *Id.* at ¶¶ 14, 16-17.

fundamental flaw in the Commission's approach. It makes little sense to try to sort out these complex technical questions in the context of trying to create "interim steps as an important bridge to the implementation of a successor technology."[16] Indeed, the Commission runs a very high risk that it will be building an interim bridge to nowhere.

Finally, BBT has no reason to comment on the Commission's inquiry regarding CableCARD installations. If a cable operator chooses to roll out a *BBTSolution*-enabled system, there are no special installation parameters. Downloadable security is accomplished in the chip set built into the device used for reception, be that a set-top box, a consumer electronics device like TiVo (if it were BBT enabled) or any other end user device such as a DVD, Blu-ray player, game console, television set or the like.

The same is true for IP "over the top" delivery or IPTV applications; all of these devices, once *BBTSolution*-enabled, could then have whatever "conditional access" the operator or programmer was using downloaded to them. There would be no distinction whatever between devices purchased by consumers and devices provided by the cable operator. "Installation," to the degree it was required, would be hooking the physical cable connection, modem Wi-Fi, or whatever to the given device. All security functions in a two-way system would then be automatic. In a one-way system the consumer may have to follow some on-screen directions, once, call the system offices and read a set of numbers (the same approach used in the initial cable modem installations). Once the secure communications path was established, all other security functions take place automatically.

---

[16] *Id.* at ¶ 13.

D. Promoting the Cable Digital Transition

As noted above, the Commission's efforts at implementing Section 629 have been marked by delay, litigation and numerous exceptions and waivers. While waivers were granted for a variety of reasons, the *FNPRM* focuses on the waivers granted by the Media Bureau "to provide cable operators with economic incentives to transition their systems to all-digital."[17] The Commission proposes to build on those waivers by allowing cable operators to place into service new, one-way navigation devices (including devices capable of processing a high definition signal) that perform both conditional access and other functions in a single integrated device (but do not perform recording functions).[18] Describing this proposal as a "limited modification" of the current rules, the Commission suggests that its adoption will allow operators to offer increased broadband speeds and more high definition programming without substantially affecting the retail market for CableCARD devices.[19]

This is not, as the Commission claims, a "limited" change. In fact, the proposed rule change would in essence eliminate the "separable security" requirement for all one-way cable navigation devices. The only "advanced" service" such devices would be restricted from providing is recording functionality. This, effectively, means that any cable system not offering "two-way" (VOD and the like) services – and there are many smaller systems nationwide that fit into that category – and all systems offering "second set" boxes that do not include "advanced services" such as DVR, would no longer have to comply with the "separable security" requirement. Given the rapid commercial adoption

[17] *Id.* at ¶ 22.

[18] *Id.*

[19] *Id.*

of "whole house" video recording devices, the single technical limitation on these newly proposed allowable set-top boxes becomes almost meaningless.

Creating such a broad, across-the-board exception to the current rules would have severe consequences for companies such as BBT that responded to the Commission's past statements encouraging the development of downloadable security solutions. For example, when the original DTA "limited" waivers were approved, market negotiations for the manufacture and sale of new technology such as the *BBTSolution*™ downloadable security nearly stopped. It had the effect of "Lucy" in the Peanuts cartoon strip pulling the ball away just as Charlie Brown was about to kick it. The reason is simple; entry into a market such as cable, with the largest operators already totally constrained by the proprietary equipment they have deployed throughout their footprints, means that the only effective entry to prove a new product (other than one designed by the large operators themselves) is in the smaller, "Tier 2" and "Tier 3" systems. But the Commission, by granting the waivers, signaled that there was a possibility things could simply continue on a well worn and proved path. Why wouldn't an operator take that option, and why would a manufacturer resist it? The Commission's action had the effect of making it that much harder to launch the new products the Commission has been seeking.

Now the Commission is proposing to create a new hurdle by establishing an across-the-board exception for one-way devices. And this time the effect of its action – which is based on reasoning that is not supportable – will be to virtually eliminate the natural growth market for new technology entry. Almost all cable systems, large and small, are delivering high definition programming today. Similarly, broadband offerings

have become a nearly ubiquitous element of the array of services offered by cable systems. Yet, the assumption seems to be that without essentially granting an industry-wide waiver for all HD-DTAs, cable systems (and, in particular, smaller systems) will not be able to afford to continue converting to digital distribution, with the result being a slowdown in the development and deployment of new broadband and high definition services. Underlying this assumption is the further assumption that compliance with the current rules requires equipment that is far more expensive than an integrated HD-DTA.

While such an assumption about the cost of compliant non-integrated equipment may have been valid when the CableCARD was the only option, the situation is much different today. Tier 2 cable operators that the Commission assumes could not afford to offer digital service without a non-compliant device have, in fact, received bids from major, established set-top box manufacturing companies willing and able to build compliant downloadable security-enabled boxes at prices in exactly the same range as the prices being quoted for non-compliant HD-DTAs.[20] Unfortunately, just the rumor that the Commission was going to either grant a broader HD-DTA waiver or would propose the broad rule change contained in this proceeding has again caused potential purchasers to hesitate just as one of the Commission's primary goals of seeing the introduction of new, compliant, separable security technology could have been consummated.

The developers of *The BBTSolution*™ downloadable security technology are themselves all small cable system operators. They are totally sympathetic to the needs of small systems, and certainly sensitive to the economic constraints small systems face.

---

[20] Because private negotiations are still underway, BBT is contractually foreclosed from disclosing specific pricing information or the parties involved.

However they believe that perpetuating the current technical *status quo* is not the right solution for cable operators, large and small.[21] Downloadable security as implemented in *The BBTSolution*™ can more than double current bandwidth usage because almost all current programming can be offered in an MPEG4 format. The headend equipment associated with *The BBTSolution*™ can be far less expensive than currently exists, and provides far more flexibility since it can offer, even to one-way systems (with less than 552 MHZ activated capacity), the ability to provide advanced services and even "*a la carte*" programming. This is all because new technology designs allow these advances. As we have just stated, those advances do not have to come at costs appreciably higher than the costs associated with the old, non-compliant technology the Commission is now considering authorizing. At this point, the more the Commission changes its rules, the more the industry, large and small systems alike, will stay the same. That is not the ultimate objective sought by Congress or the Commission.

CONCLUSION

A few weeks ago, Apple CEO Steve Jobs made a speech referencing the current set-top box market which, as the Commission itself has noted, is essentially frozen. He reportedly said: "The only way that's ever going to change is if you can go back to square one and tear up the set-top box and redesign it from scratch and...get it to the consumer in

[21] The Commission asks whether limiting the rule change to "smaller systems" with activated capacity of 552 MHz or less would make a difference regarding impact on potential CableCARD sales, but as we noted above, CableCARD UDCP devices are already increasingly scarce, and this proceeding, regardless of its outcome, has assured that very few new CableCARD devices are likely to be developed. Thus the question is not whether there will be an impact on CableCARDs, but whether the entire notion of separable security as a mechanism to open up the device market can work. We think it can, with downloadable security, and we intend to expand on that concept in the "AllVid" proceeding.

a way that they're willing to pay for it."[22] We believe that Mr. Jobs is right. However, the real question is what is "square one"? As BBT has discussed herein, the CableCARD "reforms" proposed in the *FNPRM* presume to know the answer to the question of what a "set-top" box will be in the future and whether it can and will be available in the retail marketplace – it will be an "AllVid" device.

However, BBT believes that there is another way to get back to "square one" – namely the deployment of a neutral, minimalist downloadable security approach that can technically be introduced and migrated to without disrupting the infrastructure currently deployed. Which direction most clearly fulfills the goals laid out by Congress in Section 629 and pursued by the Commission for over a decade is at the core of both the instant *FNPRM* and the related *AllVid NOI* proceeding. The complex considerations and interactions between what is done in the *FNPRM* and what might be done based on the input received by the Commission in the *AllVid NOI* proceeding cannot logically be separated and thus, as described herein, we urge the Commission to stand down from adopting the proposed revisions to its CableCARD rules until after it has completed the *AllVid NOI* and any rulemakings arising therefrom.

---

[22] Gary Arlen, "Apple's Jobs: Cable's Set-top Box Stranglehold Stifles Innovation," *Multichannel News*, June 2, 2010, available at http://www.multichannel.com/article/453241-Apple_s_Jobs_Cable_s_Set_Top_Box_Stranglehold_Stifles_Innovation.php

Respectfully submitted,

BEYOND BROADBAND TECHNOLOGY, LLC

/s/ William D. Bauer/SS

William D. Bauer, CEO/CTO
Beyond Broadband Technology, LLC
1140 10th St.
Gearing, NE 69341

Stephen R. Effros
Effros Communications
PO Box 8
Clifton, VA 20124
steve@bbtsolution.com
703-631-2099

June 14, 2010

209914

Beyond Broadband Technology / The BBT*Solution*™

A "WHITE PAPER" ON A NEW CONCEPT FOR SECURING THE TRANSMISSION OF ELECTRONIC INFORMATION

Beyond Broadband Technology, LLC, (BBT™) has developed The BBTSolution, an open standard downloadable security system (OSDS™) which does not require the use of a "trusted authority". The BBTSolution constitutes a unique method of establishing a secure communications path with either one-way or two-way devices as well as mechanisms for establishing authentication, authorization and reception of encrypted transmissions of voice, video or other data.

Explaining a new concept in the field of information security is never easy. That's particularly the case since various users, purveyors, government regulators and even standards-setting bodies use either very similar or very conflicting definitions for similar terms. This "White Paper" is meant to make clear what we are referring to with the terms being used to explain the BBTSolution, and thereby help to underscore the unique flexibility it can bring to multiple forms of information security.

INFORMATION SECURITY

This is a very broad term, and in the context of the BBTSolution, it is meant that way. The BBTSolution establishes a highly secure communications path between a transmitting device and a receiving device. The transmission medium is not restricted. As is explained below, the BBTSolution was first designed for use with cable television broadband systems. However this OSDS (open standard downloadable security system) is not restricted to any particular communications path, and will also work on IP (Internet Protocol) systems or over-the-air, satellite or other transmission paths just as well. Once a secure, authorized and authenticated communications path is established, the system is totally agnostic to the type of data, or information, transmitted over that path. Thus when we talk about "information security," it could be anything from a television program or channel, or first-run movie to health care or banking information, automated data for controlling the power grid, or any other type of information.

Once the secure communications path is established, the level of security, including authentication, usage restrictions, or any other type of security is user-definable. What makes this approach unique is that because it is "downloadable," security conditions can be changed repeatedly, depending on the use. In other words it can be employed by multiple transmitters of information, each utilizing different types and levels of security. A consumer with a BBTSolution enabled computer (either built-in or in a portable USB "dongle") for instance, could securely access multiple video programmers via the Internet, each with it's own encryption and conditional access protocols. A Veteran could have similar access to all his or her medical records at multiple locations with total security provided by a BBTSolution chip in a USB thumb-drive type device, or embedded in medical facility computers.

THE BASICS

The BBTSolution has two parts; a secure microchip in the receiving device, and an "HSM" (Hardware Security Module) at the transmitting site. The HSM can be integrated into the transmitting location of a cable broadband, satellite, broadcast or telephone system, or it could be a part of any computer server used by a provider of information on the Internet, for instance. HSM's could also be integrated into

devices (such as a host computer) used by doctors or hospitals to transmit patient data or any other data transmission application. The cost of the HSM enabled equipment will vary depending on the use. The current design for cable television systems, including the computer, costs less than $10,000, approximately one-tenth the price of the conditional access headend controllers commonly used in that market today. We anticipate that the basic Hardware Security Module enabled for use on computer servers can cost half that, or even less.

The secure microchip can be incorporated into, as examples, a cable television set-top box, a television set, a digital video recorder, a home, office or laptop computer, or even in a portable USB device (much like a "thumb drive" or "dongle") that could be inserted in any current computer USB port. The chips, which are already being manufactured by one of the best-known secure microprocessor manufacturers in the world, ST-Micro, are inexpensive (they are currently priced at $5.00 including the BBT license fee) and are designed to be integrated into multiple consumer devices, much like the well-known "Dolby™" system is included in most consumer audio devices today.

BOTH TWO-WAY AND ONE-WAY DEVICES

One of the many unique aspects of the BBTSolution is that the receiving device, such as a television set, need not be a "two-way" device. The secure communications path, once established, is totally managed by the transmitting and receiving devices themselves, and the receiving device does not have to be in constant return-path communication with the transmitting HSM enabled equipment. Thus, for instance, with one telephone call a cable television consumer could read a series of numbers that appeared on their television screen to the headend and from that point on the cable HSM enabled headend controller and the consumer's BBTSolution device can establish and maintain a secure authenticated channel (SAC) without the need for two-way communication or bandwidth use. Of course the system will also work, automatically, with two-way communications, such as with IP computer communications on the Internet or in two-way broadband cable systems.

THE ORIGINAL CHALLENGE

The BBT*Solution* was originally designed to respond to a need for a new, low-cost cable television set-top box that could meet government mandates for "separable security" for such devices. Until June of 2007, cable television systems traditionally used a set-top box (a tuner, and descrambler) that had "integrated security". That is, the entire process of assuring that the box belonged to the right customer, was in the right location, and had the proper codes to decrypt only that programming meant for that customer was all integrated into the set-top box. Legislation intended to foster a consumer market for set-top boxes resulted in the FCC establishing rules requiring that the security function be separated from the rest of the functions of the set-top box. This, theoretically, would allow anyone to design new and competitive set-top boxes that could be used in any cable system since the security function was not integrated into the box and could be enabled in each location (which had different security, or "conditional access" systems) another way.

The method originally chosen for this separated function was the CableCARD, a modified version of the PCMCIA (Personal Computer Memory Card International Association) card then in use in personal computers. The idea was that any set-top box could be built with a capability to accept the CableCARD, and that cable systems could supply the appropriate card, which controlled the security, or what has generally been called the "conditional access" components of the system. Unfortunately, CableCARDs are both expensive (both the card and the docking device) and no longer constitute an advanced technology. The PCMCIA design is generally now considered obsolete, and most computers

today no longer incorporate PCMCIA slots, having progressed to new designs such as USB (Universal Serial Bus). The BBTSolution is, however, "backward compatible" with CableCARDS.
One of the original objectives of BBT was to design a new "separable security" system. Several efforts to design such a new system were launched by various companies. Unfortunately, the layman's language used to describe these systems, which was subsequently adopted by the FCC, was "downloadable conditional access systems" or DCAS. We say unfortunate, because this language necessarily confuses the various functions being described, and implies that they are all part of a single, integrated process. While that is a traditional approach to security and conditional access, it is not the only way it can be accomplished. Another of the unique attributes of the BBTSolution is that it separates the establishment of a secure communications path from the other functions of authorization, authentication and encryption /decryption of the data. This allows, as is explained below, almost unlimited flexibility in the use of the system.

A SECURE COMMUNICATIONS PATH -- WITHOUT THE NEED FOR A "TRUSTED AUTHORITY"

The traditional approach to establishing a secure communications path is to use a "public/private encryption key" dialog between devices. However this standard approach also requires that the "private key" be in some way secured and archived for referral and use to authorize the communication. Thus, there must be a "trusted authority" holding and controlling all of the private keys. If those keys are somehow discovered, the entire security system, including all the devices with hardware linked to those keys, if any, are compromised. The BBTSolution does not employ public/private keys or require a "trusted authority," thus eliminating the two most significant drawbacks of the traditional approach.

With the BBTSolution, the "public/private" keys that enable devices to securely communicate are replaced by a "symmetrical key" approach. Keys are determined internally by the HSM and the secure micro embedded in the receiving device. Each time the HSM and a receiving device establish a secure communications link new random keys are used, thus there is no need for a "trusted authority" and the risk factor of "hacked" or stolen keys is eliminated. No user needs to rely on any other entity for the maintenance of security of the devices used in its communications. This, in turn, significantly reduces the "threat target" for secure communications. Since each user of the BBTSolution establishes their own conditions for authentication and use, what we term "conditional access," the two parts of the security protocol; establishing the secure communications path and then establishing the authentication, access and use conditions, become additive in their security effect, particularly since they are not static.

DOWNLOADABLE CONDITIONAL ACCESS

The basic BBTSolution does not include "conditional access" protocols. The entire idea behind the early development of this approach, as noted above, was to separate the establishment of the secure communications path from the conditions imposed on the use of data after that communications path was created. Thus the BBTSolution has been designed in an "open" format where specifications will be made available so that anyone can design "conditional access" software that can be downloaded to the receiving BBTSolution-enabled device. This conditional access software can be as simple or as robust as the user chooses. For instance, in the case of a cable television system operator, the conditional access system might be automatically triggered by a known subscriber code number, pin number, or location address. In the case of a portable USB "stick", which could be inserted in any modern computer at any location, a program supplier (ESPN or a movie supplier, as examples) could, once the secure communications path is established, download a customized "conditional access"

protocol that required a password, a credit card verification, or some other method of authentication. The relationship between the information provider and the customer over the Internet would be direct, and totally controlled by the conditions imposed by the intellectual property owner. In the case of medical records, it has already been suggested that the USB key or an embedded secure micro at the medical facility could be conditioned to be authorized only with thumb print verification as well as a password to assure security and privacy of personal data.

Once the BBTSolution secure communications path is established, the conditional access protocol of the given information provider is downloaded, and authentication has taken place, then the information distributor can additionally impose any other conditions for the access of the material being sent. Of course at minimum, that information is encrypted. The BBTSolution secure micro includes a "virtual machine" or "tool box" that contains over a dozen of the most commonly used encryption algorithms. These algorithms have all withstood the test of time and have proved to be highly secure. But in the BBTSolution approach they are even more so, because they can be used in any order and any combination, again at the discretion of the information provider. Thus a conditional access protocol could be downloaded instructing the BBTSolution secure micro to use, assuming, for instance, if there were 12 algorithms available, any combination of 12 to the 12^{th} power combination of encryption/decryption processes. However one can never assume that something simply can never be "broken," so the system is designed so that the protocol can be changed at will by the provider, as many times as they wish, and as often as they choose. It is generally acknowledged that a "software-only (DRM--"digital rights management") approach to encryption or conditional access is subject to constant challenge. As the saying goes, "..there's a new crop of 18-year-old hackers every year!" The BBTSolution HSM and microchip, along with a downloadable conditional access component, does not suffer from that same risk. It is a highly adaptable, nimble and very flexible approach to secure communications.

Along with establishing security and conditional access, including any form of additional "DRM" chosen by the information provider, the ability to "download" protocols allows for other flexibility as well. For instance information stored in different formats may require that a "reader" be associated with the information being transmitted. This is particularly true in a field such as health care. Reader programs, with limitations on use, both in terms of time and content, could be downloaded and deleted with each session establishing a secure communications path. Data downloaded to a computer hard drive could be stored only in encrypted form, thus totally protected unless a secure communications path was established to authorize decryption.

CONCLUSION

The BBTSolution is unique. It allows for absolutely secure communication and control of intellectual property and privacy of data transmissions on multiple broadband and narrowband formats. It can enable such communication to devices that are either one-way or two-way capable. It does not require a "trusted authority" and allows for maximum flexibility for individualized conditional access and use. It's potential uses for broadband and the Internet , in particular, can fundamentally change the way those platforms are used today.

ADDENDUM ATTACHED

ADDENDUM – January, 2010

Recent events have highlighted, once again, the validity of the reasoning behind the BBTSolution™ approach to electronic information and communications security. The experimental "hacking" of the latest proposed algorithm for use in 3G cellular telephony and the increased focus on illegal international efforts to access proprietary data from various secure repositories of corporate information has once again demonstrated the weakness in current security thinking. Software solutions and "secure repositories" or "trusted authorities" are being challenged regularly and there is no indication that this activity will stop. Indeed, it clearly is increasing.

The BBTSolution™ answer to that challenge is a design where any attack on the system is anticipated, repairable, and totally limited. There is no "trusted authority." The "threat target" in the BBT approach can be reduced, literally, to single communications events. Each initiation of the BBTSolution™ secure communications path utilizes a totally unique and individualized creation of ephemeral keys. Those keys would have to be broken during the communications session, since once the individual session is over those keys are no longer of any relevance. Further, since each session and associated conditional access protocol is totally controlled (as to timing, duration, content, encryption, etc.,) by the communicating parties, they can change any or all parameters at will. A "hacker" would have to, while the communications session was in progress, ascertain all of those variables, including the methodology and algorithm used for deriving the unique session keys. Portions of that methodology and the algorithms used are variable as well, making any single session "hack" of very limited value.

Rather than try to create a "Fort Knox" that "can't be broken into," BBT has taken a totally different approach, creating a security design that is so nimble and flexible that the extreme effort it would take to compromise the secure communications path could only yield a result, if successful at all, for that single, unique communication. In addition, all system administrators create their own set of variables, encryption and additional conditional access protocols, adding to the overall security of the vast majority of uses.

A REPRESENTATIVE EXAMPLE: ELECTRONIC MEDICAL RECORDS

There are several interrelated issues in the effort to shift to electronic medical records. Not only is individual security and privacy required, but the records themselves, as in the case with the Veterans Administration, for example, may be in different locations and they may not all be uniform. The use of the BBTSolution™ downloadable security design can address all of those challenges.

In order to assure privacy and authentication, a BBTSolution™ secure microchip can be embedded in a personal "USB Dongle" (a form-factor like a "thumb drive") which also incorporates a biometric (thumb print) reader. The veteran could then visit any facility with computers having USB inputs and authenticate his or her right to access the particular medical records by establishing a secure communications path with any repository medical computer having the requisite HSM (Hardware Security Module). The encrypted thumb print data is stored directly on the resident secure microchip. The USB device will not establish any secure communication without that initial authentication. Any additional authentication required, such as a password, an account number or whatever the institution requires with its own pre-established set of conditional access rules, which would be downloaded to the receiving computer upon initiation of the secure communications path, would assure that the encrypted records were only being transmitted to the appropriate location and that only that location had the requisite information to decrypt the files. That decryption capability would, in this example, only last as

long as the secure communications path was in place.

The process also anticipates the interim "downloading" of specialized software should the sending and receiving medical facility not have the same capabilities for reading or reviewing the records. It, too, would only be useable so long as the secure communication path was intact, or limited in any other way decided upon.

Of course any other set of variables could be applied to the medical data thus downloaded. It could be time limited and then automatically discarded, it could be decrypted or left entirely encrypted and only accessible during secure communications path sessions with the personalized USB key, or it could be authorized for use by the new medical facility as a repository for the data. All of these options and many more can be made available through the use of easily developed and downloaded computer code. The key to the secure communication of the data is the initialization of the secure communications path, and the multiple options afforded the user through downloadable capability once that path is established.

While we have cited a USB thumb-drive type form factor (currently tested and ready for mass production) in this quick exploration of how the BBTSolution™ can be used to address many of the challenges of electronic health care records security and distribution, there are other form factors that could also be employed, such as a "smart card," or the BBT secure microchip being directly incorporated into a computer laptop. In addition, it should be noted, again, that because of the flexibility inherent in the downlaodable design, the same chip (in whatever form factor) used for securing electronic medical records, for instance, could also be used to view a movie, download a book, or do anything else requiring an authenticated secure communications path to multiple devices such as computers, laptops, television sets, game consoles, etc.

The whole point behind this (patent pending) approach to broadband IP security is that it can be used for multiple purposes and each one can be secured in a different way with as much or as little additional conditional access as is deemed necessary by the parties establishing the communications path. Each communications session is unique as to use, content, authentication and any other conditions chosen based on the nature and need of the communicating parties. Because of that flexibility and versatility, the BBTSolution™ security protocol enables far more uses in a more secure manner than current designs.

03 05 10

Contact: Steve Effros
steve@bbtsolution.com
703-631-2099